IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

UNITED STATES OF AMERICA)	CASE NO. 1:16CR308-1
)	
vs.)	
)	Winston-Salem, North Carolina
KYLE EDWARD MASCETTI)	October 24, 2016
	11:00 a.m.

TRANSCRIPT OF THE **RULING ON MOTION TO SUPPRESS**
BEFORE THE HONORABLE THOMAS D. SCHROEDER
UNITED STATES DISTRICT JUDGE

APPEARANCES:

For the Government: ERIC L. IVERSON, AUSA
Office of the U.S. Attorney
101 S. Edgeworth Street, 4th Floor
Greensboro, North Carolina 27401

For the Defendant: KATHLEEN A. GLEASON, AFPD
Office of the Federal Public Defender
301 N. Elm Street, Suite 410
Greensboro, North Carolina 27401

Court Reporter: BRIANA NESBIT, RPR
Official Court Reporter
P.O. Box 20991
Winston-Salem, North Carolina 27120

Proceedings recorded by mechanical stenotype reporter.
Transcript produced by computer-aided transcription.

P R O C E E D I N G S

(The Defendant was present.)

MR. IVERSON: Good morning, Your Honor. Mr. Iverson for the Government. The matter before Your Honor is United States versus Kyle Edward Mascetti, 1:16CR308-1. Mr. Mascetti is present with his counsel, Ms. Gleason. This matter is on for a decision on the suppression hearing.

MS. GLEASON: Good morning, Your Honor.

THE COURT: Mr. Mascetti, good morning.

THE DEFENDANT: Good morning.

THE COURT: I noticed the Government filed a supplement shortly after the hearing. It looked like it was with the consent of the Defendant. Is there anything further that's been filed after that? I have not seen anything.

MS. GLEASON: No, Your Honor.

THE COURT: Okay. I decided to just rule from the bench rather than to write a written opinion in this matter. So my ruling is going to take quite some time, so let me go through that.

Let me indicate, for the record, the Defendant is charged in a two-count indictment with receiving and attempting to receive child pornography in violation of Title 18 of the U.S. Code, Section 2252A, paragraph (a)(2)(A), and with accessing with intent to view child pornography in violation of Title 18 of the U.S. Code, Section 2252A, paragraph (a)(5)(B).

The motions before the Court are a motion to dismiss and a motion to suppress. They have been briefed, and the Court held a hearing on October 6, 2016.

Let me start with the motion to dismiss the indictment. I think I indicated last time I was not inclined to grant that motion, and that is, in fact, my decision on that. The Government has responded, including with sealed exhibits.

The Defendant is moving to dismiss the indictment on the ground that the Government committed and facilitated the crimes charged here because the Government ran the Playpen website for approximately two weeks after it seized it in 2015. The Defendant argues that the Government's conduct is outrageous and warrants dismissal. The Defendant argues that the Government both facilitated the distribution of child pornography and caused harm to innocent third parties, the victims of the child pornography.

The U.S.'s response is essentially that the Government's conduct was neither unreasonable nor outrageous, the Government contends, because it was the only way for the Government to determine who was accessing the Playpen website and that the Government limited the duration of its use of the website for about two weeks.

In *Rochin v. California*, 342 US 165, and in *U.S. v. Russell*, 411 US 423, the Supreme Court reiterated the principle that due process may be violated where the conduct of the

Government is so outrageous that it "shocks the conscience" and violates the standards of decency and fairness so as to "bar the Government from invoking judicial processes."

As the Fourth Circuit said in *U.S. v. Hasan*, 718 F.3d 338, the Government conduct must reach the level of being "shocking" or "offensive to traditional notions of fundamental fairness," or as the Fourth Circuit said in *U.S. v. Goodwin*, 854 F.2d 33, the Defendant must demonstrate that the conduct of the Government was "outrageous, not merely offensive."

Here, the Court finds that the Government's conduct can be described as, in fact, unsavory. It may even be questionable, but it's not so outrageous as to shock the conscience of the Court. The Government did not create the Defendant's crimes. The Defendant decided to seek out the child pornography, and he had to take several affirmative, intentional, and knowing steps in order to reach that point, including seeking out the Playpen website whose location is not generally available, entering a unique user name and password, and accessing a child pornography post within the forum listed on the website. Only then was the Network Investigative Technique, otherwise known as the NIT, installed in this case.

Given the anonymity of the Playpen site, the Government's conduct is understandable and was likely necessary to identify those who were users of the site and receiving child pornography. There is no indication that the Government's mere

seizure of the website provided it with the information sufficient to identify those who were using it. The Government's use was also limited in time.

As the Court said in *U.S. v. Allain*, 15CR10251, from the District of Massachusetts, "As child pornography migrates to the hidden corners of the web, the Government will have to continue to make difficult choices about how to investigate and prosecute the related crimes. Reasonable minds will no doubt differ on whether the Government made the right choice here, but it is not the rare case in which any misconduct on the part of the Government was sufficiently blatant, outrageous, egregious to warrant the dismissal of the indictment."

So the motion to dismiss the indictment, which is Doc. 17 in the record, is denied.

That takes me then to the motion to suppress. The Defendant moves to suppress all evidence from the search of his home computer and the fruits of the search. That's Document 15. The Government has responded and has submitted a supplemental response, and the Court has read all of those, including a number of cases cited in support and in response of the motion.

The Defendant's moving to suppress on several grounds. The key grounds are as follows:

First, that the warrant lacked probable cause.

Second, that the warrant was an anticipatory warrant whose

triggering event did not occur.

Third, the search of the Defendant's computer in North Carolina exceeded the scope of the warrant, which is argued to have been limited to the Eastern District of Virginia.

And, fourth, even if the warrant authorized searches outside of the Eastern District of Virginia, its issuance violated Federal Rule of Criminal Procedure 41.

I'll note for the record that the Defendant is not pressing any argument or request for a hearing under *Franks v. Delaware*.

Let me address probable cause. The Defendant contends that the warrant lacked probable cause. The Defendant argues that the object of the warrant, the Playpen website, which is accessed through the secure and essentially anonymous "onion," otherwise known as the Tor network, The Onion Router network, contained both legal and illegal, that is, child pornography, material. Therefore, the Defendant argues principally that the warrant was overboard inasmuch as it authorized the FBI to search any user who logged into the site regardless of whether he or she sought illegal content.

The United States argues that the warrant was supported by probable cause, that the Playpen site was dedicated to child pornography, and that there were grounds for the magistrate judge to conclude there was a fair probability that anyone who logged into the site did so with the knowledge of its illegal

content and an intent to access that.

The Court finds the following: That is, that the Tor network, by design, provides anonymity to users; that the Tor network is used by criminals and for their online sexual exploitation of children, in particular; that to use the Tor network with anonymity, users must purposefully download software for it. Tor is designed to prevent others from identifying a user's IP address for the user's personal computer, which it does, in part, by the manner it routes communications through other computers.

The Court also finds that the Playpen site is a hidden site. That is, a user cannot find it by conducting a Google-type search. Rather, a user must first obtain Playpen's specific web address from another source, such as online postings or from other Playpen users. The Court finds that accessing Playpen requires numerous steps, including obtaining a user name and a password.

As noted in the supporting warrant affidavit, Playpen was "dedicated to the advertisement and distribution of child pornography." It was described to contain "discussion of methods and tactics offenders use to abuse children" and "methods and tactics offenders use to avoid law enforcement detection while perpetrating online child sexual exploitation crimes," and it was explained that "administrators and users of Playpen regularly send and receive illegal child pornography

via the website."

Facts that support this description contained in the affidavit:

The main page of the site at the time of the affidavit displayed partially clothed prepubescent females with their legs spread apart, the phrases adjacent to the pictures said "no cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace Out," and the images revealed Playpen as a hub for trafficking illicit child pornography.

The Court finds that the vast majority of the sections, forums, and subforums noted on the website clearly indicate the presence of illegal child pornography with such titles as "hard core," and they are divided in "girls" and "boys."

The Court finds that the warrant was supported by probable cause. The Fourth Amendment to the U.S. Constitution provides that the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures shall not be violated, and no warrants shall issue but upon probable cause supported by oath or affirmation and particularly describing the place to be searched and the persons or things to be seized.

As the Supreme Court said in *Illinois v. Gates*, "probable cause is a fluid concept, turning on the assessment of probabilities, in particular, factual contexts, not readily, or even usually, reduced to a neat set of legal rules."

A magistrate judge considering whether probable cause supports the issuance of a search warrant must "make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him or her, including the veracity and basis of knowledge of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place." That's from *Illinois v. Gates*.

A warrant application's supporting affidavit must be more than conclusory and bare bones; indeed, it "must provide the magistrate with a substantial basis for determining the existence of probable cause."

Probable cause is not subject to a precise definition. When examining an affidavit, a magistrate judge may rely on law enforcement officers who "draw on their own experience and specialized training to make inferences from and deductions about the cumulative information available to them that might well elude an untrained person," as long as the affidavit contains facts to support the officer's conclusions. That's supported by *U.S. v. Johnson*, 519 F.3d 339 at page 343.

This Court should afford the magistrate's determination of probable cause great deference. Therefore, this Court's duty is "to ensure that the magistrate had a substantial basis for concluding that probable cause existed," as the Court indicated in *Illinois v. Gates* at page 238 to 239. A reviewing court

should "resist the temptation to invalidate warrants by interpreting affidavits in a hypertechnical, rather than commonsense, manner," as the Court noted in the Fourth Circuit in *U.S. v. Blackwood*, 914 F.2d at page 142.

At the outset, I will note that there is a substantial question in my mind whether a user has a reasonable expectation of privacy in his or her IP address. Users regularly make their IP address public when using the Internet. The issue here, though, is whether the use of the Tor network created a reasonable expectation of privacy inasmuch as the network is designed to protect anonymity, but the Court need not reach this issue because the totality of the circumstances show that even if there was a reasonable expectation of privacy in the information the NIT revealed, a fair probability existed that those accessing Playpen intended to view and trade child pornography and that the NIT would help uncover evidence of these crimes.

The warrant affidavit describes the Tor network, its emphasis on anonymity, the need for knowledge of its web location and address, the need for separate user name and password, and an advisory to users to use a false email address. It is unlikely that an unwary Internet traveler would find the website and use it accidentally.

References on the Playpen website show that it is dedicated to child pornography. Its images, its filenames, the

vast majority, are categorized repositories for child pornography, subdivided by gender and age of the victims, and the directions about types of files that can be loaded onto it. The warrant affidavit described how users engage in child pornography private messages on Playpen to disseminate child pornography.

So the Court finds under the totality of circumstances that the magistrate judge did have probable cause to issue the NIT warrant. I will note this decision is consistent with that of a host of other courts that are cited in Document 22 at page 24.

The next argument raised by the Defendant is that the warrant was an anticipatory warrant whose triggering event that would establish probable cause never occurred. The Defendant argues that the triggering event was visiting Playpen's homepage and that this never occurred because the FBI included a false description of the homepage in its application for the warrant. The Defendant argues it was false because the homepage changed to an innocuous image between the time the application was made and two days later when it was signed. The Defendant argues that the search in his case, therefore, exceeded the scope of the warrant.

The U.S. contends that the triggering event was not visiting the site but entering a user name and password. It also argues that the NIT was not deployed until the Defendant

later accessed a particular section containing the child pornography, that is, a section entitled "Girls HC," meaning hard core, and, according to the supplemental materials filed by the Government, when the Defendant opened a post within that forum.

In *United States v. Grubbs* at 547 U.S. 90 at page 94, the Supreme Court concluded that anticipatory warrants are "based upon an affidavit showing probable cause that at some future time, but not presently, certain evidence of a crime will be located at a specified place." The Court noted that these -- generally these warrants "subject their execution to some condition precedent other than the mere passage of time, a so-called triggering condition."

Once the triggering event occurs, there is reason to believe the item described in the warrant would be present. Otherwise, "if the Government were to execute an anticipatory warrant before the triggering condition occurred, there would be no reason to believe the item described in the warrant could be found at the searched location; by definition, the triggering condition which establishes probable cause has not yet been satisfied when the warrant is issued."

Thus, as the Court said in *Grubbs*, it "must be true not only that if the triggering condition occurs, there is a fair probability that contraband or evidence of a crime will be found in a particular place, but also that there is probable

cause to believe the triggering condition will occur." "The Fourth Amendment does not require that the triggering condition for an anticipatory search warrant be set forth in the warrant itself," according to *U.S. v. Grubbs* at page 99.

Here, the Court finds that the triggering event was not visiting the web page of Playpen but logging into the site with a user name and password. Thus, the Defendant's argument that the image on the web page having been changed at the last minute does not change the analysis. The Court also finds that in this case the FBI did not employ the NIT until the Defendant took the additional step of accessing a post within a particular section of this site known to contain child pornography.

The Defendant's challenge to the warrant on this ground is therefore denied.

The Defendant next argues that the search warrant was issued only in the Eastern District of Virginia, and it authorized searches only in that district. Because the Defendant's computer was located in North Carolina, it is argued the Government exceeded the scope of the warrant and the good-faith exception would not apply.

The U.S. argues that the warrant application made clear how the NIT would be deployed, that is, that it would be deployed in the Eastern District of Virginia to a computer that accesses the Playpen site maintained on the server in the

Eastern District of Virginia, and then it would obtain identifying information from the computer logged into the site no matter where it was located.

The Court agrees with the Government. The warrant, Attachment A, made clear that the warrant authorized the use of the NIT on those who accessed the Playpen website and that the NIT would be activated on "those of any user or administrator who logs into the target website using a user name and password."

This is consistent with the affidavit supporting the warrant, which specifically requested authority for the NIT to "cause an activated computer, wherever located, to send a computer controlled by or known to the Government messages containing information that may assist in identifying the computer, its location, other information about the computer and the user of the computer." That's the affidavit, paragraph 46(a).

The reasonable and fair reading of the warrant application and affidavit are that the Government sought permission to deploy the NIT in the Eastern District of Virginia onto any computer, wherever located, that logged into the site. Thus, the Defendant's challenge on that basis is denied.

The next issue is whether Rule 41 of the Federal Rules of Criminal Procedure authorized the NIT warrant to

issue. The Defendant argues that even if the warrant authorized searches outside of the Eastern District of Virginia, the warrant exceeded the magistrate judge's scope of authority under Federal Rule of Criminal Procedure 41 and that the good-faith exception does not apply.

The U.S. argues that the NIT warrant was authorized by Rule 41(b), and in any event, the search here is covered by the good-faith exception under *Leon*. The authority of a magistrate judge to issue a warrant is covered by both Rule 41 and the magistrate judge's enabling statutory authority set out in 28, U.S. Code, Section 636. As the Court noted in *U.S. v. Matish*, 2016 WL 3455776, the provisions are intertwined.

Section 636 grants the magistrate judge authority set out by law and by the Rules of Criminal Procedure. Rule 41(b) grants magistrate judges authority to issue warrants under several scenarios. The United States argues that three provisions of the rule apply here: Rule 41(b)(1), (b)(2), and (b)(4). The Government focuses on Rule 41(b)(4), which provides "a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both." A tracking device is defined by Rule 41(a)(2)(E) to be "an electronic or mechanical device which permits the tracking of the movement of a person

or object."

The Defendant cites two decisions that have concluded that the NIT is not like a tracking device and, thus, exceeded Rule 41. The Government cites cases holding to the contrary.

The Court concludes that the more persuasive cases are those that are cited by the Government. The Court would, therefore, conclude that the NIT operated, in effect, like a tracking device under 41(b)(4). The NIT was installed in the Eastern District of Virginia on the electronic signal sent by the Defendant to the Playpen server in the Eastern District of Virginia when the Defendant requested that the Playpen server deliver other information, here, child pornography, to him. The Defendant made a virtual trip to the Eastern District of Virginia with his electronic request to the Playpen server. While the Playpen post was being downloaded, the NIT sent its information to the FBI on the same connection used by the Defendant to retrieve the contraband, child pornography. So the NIT identifies the source of the signal that has reached into the Eastern District of Virginia and the Playpen website.

Notably, Rule 41(a)(2)(A) defines property for purposes of the tracking device to include as well information. So the NIT is permitting the Government to track the movement of the electronic information, here, the Playpen forum information about child pornography, requested by a user. In some ways, the NIT may be less intrusive than a tracking

device, but the NIT identifies the location of the information insofar as it is sent to the recipient's computer. A mobile tracking device, by contrast, follows the vehicle wherever it goes.

Having reached this conclusion, the Court need not reach the Government's other arguments under Rule 41, including the argument that Rule 41 should be read broadly to allow warrants not expressly allowed by the rule. However, I do find that even if Rule 41 did not authorize the warrant, and certainly reasonable minds might differ on that, there are cases going both ways. I would find and do find that the search was justified by the good-faith exception to the warrant requirement set forth in *U.S. v. Leon* at 468 U.S. 897.

In *U.S. v. Leon*, the Supreme Court established a good-faith exception to the exclusionary rule. Under the exception, a Court need not exclude evidence obtained pursuant to a later-invalidated search warrant if law enforcement's reliance on the warrant was objectively reasonable, as noted by the Fourth Circuit in *U.S. v. Doyle*, 650 F.3d at 467.

There are four exceptions to this rule:

The first is if the issuing magistrate judge is misled by information in the affidavit that the affiant knows or should know is false.

The second is if the issuing magistrate judge completely abandons his or her judicial role.

The third is if the affidavit includes so little indicia of probable cause that official believe in its existence is entirely unreasonable.

And the fourth is if the warrant is so facially deficient that the executing officer cannot reasonably presume it to be valid.

All of these are set out in *U.S. v. Leon* at page 923.

Here, the agents' reliance on the NIT warrant was objectively reasonable, and the agents acted in good faith. An experienced and neutral magistrate judge reviewed the warrant application, and the magistrate judge concluded that probable cause existed to issue the NIT warrant.

None of the exceptions to the *Leon* rule apply here. There is no evidence that the FBI intentionally or recklessly misled the magistrate judge in its quest to obtain the NIT warrant, either on the scope of the warrant or in the information concerning the logo change.

The warrant application detailed ample probable cause to support the warrant, as I've already noted. The affidavit also adequately described the items to be seized and the places to be searched. There is also no indication that the FBI engaged in any type of improper conduct or had any misjudgment in relying on the NIT warrant. There is no evidence that the magistrate judge abandoned her judicial role or failed to read the warrant application and warrant carefully. Nor is the

warrant full of boilerplate; rather, it is particularized to the situation at hand.

The Defendant argues that the magistrate judge should have shown that the warrant would exceed Rule 41, and the Court disagrees. In fact, there are many courts that have found that the warrant is, in fact, covered by Rule 41, and the fact that many courts have reached this conclusion is simply further proof that law enforcement officers would have been reasonable to have relied on the magistrate judge's issuance of the warrant, and that it was authorized.

Accordingly, even if the deployment of the NIT exceeded Rule 41 -- as I said, reasonable minds may differ on that -- I would find that it would not be appropriate to suppress the information in this case because of the fact that the officers acted in good faith and the *Leon* exception would apply.

So having considered -- I believe I've covered the principal arguments raised here, but having considered all the arguments raised in the briefing, for these reasons, the motion to suppress will be denied.

Anything further I need to address at this point?

MS. GLEASON: Not for the Defendant, Your Honor.

MR. IVERSON: Not from the Government, Your Honor.

THE COURT: Give me just one moment. I know that's not the result you were hoping for, Mr. Mascetti, but, unfortunately, that's my ruling in this case.

All right. Unless there is anything further then, we'll adjourn Court. Please adjourn Court.

(END OF PROCEEDINGS AT 11:30 A.M.)

******

UNITED STATES DISTRICT COURT

MIDDLE DISTRICT OF NORTH CAROLINA

CERTIFICATE OF REPORTER

I, Briana L. Nesbit, Official Court Reporter, certify that the foregoing transcript is a true and correct transcript of the proceedings in the above-entitled matter.

Dated this 9th day of November 2016.

Briana L. Nesbit, RPR
Official Court Reporter